IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.:	10/690,778	**Conf. No.:**	1597
Filing Date:	10/22/2003	**Art Unit:**	3621
Appellants:	Abe et al.	**Examiner:**	Murdough, Joshua A.
Title:	CONFIDENTIAL FRAUD DETECTION SYSTEM AND METHOD	**Docket No.:**	CHA920030025US1 (IBMC-0084)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

This is an appeal from the Final Office Action dated June 11, 2010, rejecting claims 1-3 and 5-11. The requisite fee for the Notice of Appeal set forth in 37 C.F.R. § 41.20 (b) (1) was submitted on September 7, 2010. The requisite fee for the Appeal Brief set forth in 37 C.F.R. § 41.20 (b) (2) is submitted herewith.

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There is no related appeal or interference.

STATUS OF CLAIMS

As filed, this case included claims 1-37. Claims 1-3 and 5-11 remain pending, stand rejected, and form the basis of this appeal. Claim 4 has been canceled. Claims 12-37 have been withdrawn. No claim has been allowed. The rejections of claims 1-3 and 5-11 are being appealed.

STATUS OF AMENDMENTS

No after-final amendment of claims was proposed following the Final Rejection of June 11, 2010.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention, as defined by independent claim 1, is a fraud detection system (Fig. 1, item 11) for detecting fraudulent transactions. The system (Fig. 1, item 11) comprises an interface (Fig. 1, item 16) for inputting transaction data and outputting analysis results (page 8, lines 14-21). The system (Fig. 1, item 11) comprises a tamper-resistant secure data processing unit (SDPU) (Fig. 1, item 10). The SDPU (Fig. 1, item 10) includes a security system (Fig. 1, item 18) that can restrict access to data and program execution (page 8, line 22 to page 9, line 6), an analysis system (Fig. 1, item 22) for analyzing inputted transactions (page 9, lines 7-14) and a plurality of surveillance algorithms (Fig. 1, item 28) stored in an encrypted database (page 10, lines 1-3) wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent (page 9, lines 7-14), and a selection program (Fig. 1, item 26) for selecting at each of a sequence of random times a different surveillance algorithm to be used by the analysis system (page 10, lines 1-20).

A further aspect of the present invention, as defined by claim 6 is a method for detecting fraudulent transactions (page 6, lines 10-13). The method comprises providing an interface for inputting transaction data and receiving analysis results (page 8, lines 14-21). The method comprises providing a secure data processing unit (SDPU) (Fig. 1, item 10) that provides a secret and tamper-resistant computing environment (page 8, line 22 to page 9, line 6), wherein the SDPU can restrict access to data and program execution (page 8, line 22 to page 9, line 6). The method comprises providing a plurality of surveillance algorithms stored in an encrypted database (page 10, lines 1-3). The method comprises analyzing inputted transactions for fraud with a surveillance algorithm within the SDPU(page 9, lines 7-14). The method comprises selecting a different surveillance algorithm from the plurality of surveillance algorithms for analyzing future inputted transactions (page 10, lines 1-20).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-3 and 5-11 are obvious under 35 USC § 103(a) as being unpatentable over Zeigler (US Pub. 2004/0044739), hereinafter "Zeigler", in view of Douceur et al. (US Pub. 2004/0060042), hereinafter "Douceur", and further in view of Tochikubo et al. (US Pat. 7,096,357), hereinafter "Tochikubo".

ARGUMENTS

1. Claims 1-3 and 5-11 are not obvious over Zeigler in view of Douceur and further in view of Tochikubo.

Claim 1. Appellants assert the rejection by the Examiner does not teach or suggest the invention as defined by independent claim 1. Ziegler does not show the element "a plurality of surveillance algorithms stored in an encrypted database wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent." The Examiner asserts that Zeigler teaches "a plurality of surveillance algorithms" and cites paragraph [0054]. The Examiner takes the position that the phrase "perform several securing functions" in Zeigler is equivalent to "a plurality of surveillance algorithms" in claim 1. However, paragraph [0054] of Zeigler lists the securing functions performed by the ATM shell as "generat[ing] a digital signal", "authenticat[ing] the terminal", "unload[ing] itself", "forc[ing] an upgrade", "downloading a more current version of the ATM shell", "validating itself" and "establish[ing] an SSL connection" when authentication and upgrading are completed. Appellants assert than none of the listed functions in paragraph [0054] qualifies as a surveillance algorithm. In fact, an objective reading of each of the listed securing functions of Zeigler makes clear Zeigler does not teach or suggest the element of "a plurality of surveillance algorithms stored in an encrypted database wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent." The listed securing functions of Zeigler are never used to "make a determination regarding a probability that inputted transactions are fraudulent." The securing functions of Zeigler are in no way connected to inputted transactions.

Furthermore, Zeigler specifically states that the ATM shell may unload itself if fraud is detected. There is never a determination in Zeigler by a surveillance algorithm "regarding a probability that inputted transactions are fraudulent." In fact, the ATM shell of Zeigler is a piece of software downloaded by a merchant or some other site (paragraph [0036]). The ATM

shell, after execution allows transmission of an ATM session plug-in which allows funds to be transferred from the customer to the merchant using debit networks rather than credit card networks (paragraph [0037-0045, 0125]). Zeigler never looks at inputted transactions until the terminal authentication is created (paragraph [0054-0055]), which is after the "securing functions" performed by the ATM shell. Appellants assert that Zeigler never teaches or suggests a plurality of surveillance algorithms stored in an encrypted database wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent.

In rejecting this argument, the Examiner states "Clearly 'unloading itself if fraud is detected' is something the software contains an algorithm for if determines it needs to, when the probability of fraud is 100 percent [sic]. Authenticating the terminal and validating itself are additional algorithms that that would be run to help determine if there is a probability of fraud. If the terminal does not authenticate, there is a higher probability of fraud. Similarly, if the software cannot be validated, it has been corrupted or tampered with, which would result in incorrect fraudulent transactions." This statement by the Examiner does not show the element of "a plurality of surveillance algorithms stored in an encrypted database wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent." Neither authenticating a terminal nor validating itself (ATM shell) meet the limitation of "wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent." The surveillance algorithms in Appellants' claims look at inputted transactions. The "securing functions" of Zeigler never look at "inputted transactions."

Moreover, the Examiner admits that Zeigler does not show "a selection program for selecting at each of a sequence of random times a different surveillance algorithm to be used by the analysis system." The Examiner cites Douceur as showing random selection with a predefined correlation coefficient and calculation of the coefficient from already generated random values. The Examiner concludes it would be obvious to have modified the teachings of Zeigler to add calculations and selection method of Douceur so that a comparison of the predefined rho and the calculated rho would trigger an alert as taught by Zeigler if the difference exceeded a threshold. Appellants assert the combination of Zeigler and Douceur could not produce the instant invention. As detailed above, Zeigler does not teach "a plurality of surveillance algorithms stored in an encrypted database wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent." Douceur is concerned with improving the working set of a program image (Abstract), so Douceur is not related to detecting fraud and is therefore non-analogous art. Furthermore, the random selection referred to by the Examiner is that the "*algorithm* has random selection aspects, each time the *algorithm* is invoked a different layout is typically generated (paragraph 0050]). Thus, the algorithm of Douceur is used to generate various layouts, the plurality of layouts producing a variety of program images which are used to calculate the standard deviation and normal coefficient. These values are used to determine the tradeoff between generating additional layouts and the associated computational expense versus the expectation of incremental improvement of further layouts. Thus, Douceur does not teach "a selection program for selecting at each of a sequence of random times a different surveillance algorithm to be used by the analysis system." Douceur teaches one algorithm having random

selection aspects (paragraph [0050]). Thus, the combination of Douceur and Zeigler do not render the present invention obvious.

Tochikubo is cited for showing encrypted storage of algorithms. However, Tochikubo does not correct the deficiencies of the Zeigler/Douceur combination. Therefore, Appellants assert a proper prima facie obviousness rejection has not been presented and withdrawal of the rejection is requested.

Claim 6. Appellants assert the rejection by the Examiner does not produce the invention as defined by independent claim 6. Claim 6 requires "providing a plurality of surveillance algorithms stored in an encrypted database" and "analyzing inputted transactions for fraud with a surveillance algorithm within the SDPU." The listed securing functions of Zeigler are never used to analyze "inputted transactions for fraud with a surveillance algorithm within the SDPU." As detailed above, the securing functions of Zeigler are not surveillance algorithm and are in no way connected to inputted transactions. Therefore, Appellants assert a proper prima facie obviousness rejection has not been presented with regard to independent claim 6. Zeigler does not teach the elements of "providing a plurality of surveillance algorithms stored in an encrypted database" and "analyzing inputted transactions for fraud with a surveillance algorithm within the SDPU." Douceur and Tochikubo do not teach this element. Thus, the combination of Zeigler, Douceur and Tochibuko could not produce Appellants' invention as defined by claim 6.

Claims 2, 3, 5. and 7-11. Appellants submit that each of the dependent pending claims is patentable as they rely on a patentably distinct independent claim.

In light of the above, Appellants respectfully submit that all claims are in condition for allowance. Should the Examiner or Board require anything further to place the application in

better condition for allowance, the Examiner is invited to contact Appellants' undersigned representative at the number listed below.

Respectfully submitted,

/Carl F. Ruoff/

Date: November 5, 2010

Carl F. Ruoff
Reg. No. 34,241

Hoffman Warnick LLC
75 State Street, 14th Floor
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)

CLAIMS APPENDIX

1. A fraud detection system for detecting fraudulent transactions, comprising:

an interface for inputting transaction data and outputting analysis results; and

a tamper-resistant secure data processing unit (SDPU), wherein the SDPU includes:

a security system that can restrict access to data and program execution;

an analysis system for analyzing inputted transactions;

a plurality of surveillance algorithms stored in an encrypted database wherein the plurality of surveillance algorithms make a determination regarding a probability that inputted transactions are fraudulent; and

a selection program for selecting at each of a sequence of random times a different surveillance algorithm to be used by the analysis system.

2. The fraud detection system of claim 1, wherein the SDPU further includes an algorithm performance system that assists the selection program in selecting surveillance algorithms.

3. The fraud detection system of claim 1, wherein the selection program includes a random selection program for selecting surveillance algorithms.

5. The fraud detection system of claim 1, wherein the security system includes an encryption system for encrypting and decrypting data.

6. A method for detecting fraudulent transactions, comprising:

providing an interface for inputting transaction data and receiving analysis results;

providing a secure data processing unit (SDPU) that provides a secret and tamper-resistant computing environment, wherein the SDPU can restrict access to data and program execution;

providing a plurality of surveillance algorithms stored in an encrypted database;

analyzing inputted transactions for fraud with a surveillance algorithm within the SDPU; and

selecting a different surveillance algorithm from the plurality of surveillance algorithms for analyzing future inputted transactions.

7. The method of claim 6, wherein the step of selecting a different surveillance algorithm utilizes a random selection process.

8. The method of claim 7, comprising the further steps of:

measuring algorithm performance; and

using the measured performance in selecting surveillance algorithms.

9. The method of claim 8, comprising the further steps of:

measuring a randomness of the algorithm selection process using a technique selected from the group consisting of correlation and entropy measures; and

issuing an alert if the randomness goes under a predetermined threshold.

10. The method of claim 6, wherein the SDPU prevents observation by an outside observer of which surveillance algorithm is selected.

11. The method of claim 6, including the further step of decrypting the selected surveillance algorithm.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

There is no related proceeding.